Big Brother Watch v. UK

Massimo Frigo 2021-06-04T11:00:36

On 25 May 2021, the Grand Chamber of the European Court of Human Rights issued a landmark ruling on the compatibility of systems of mass surveillance with the European Convention on Human Rights (ECHR), the essential elements of which were first brought to public light by the revelations of whistleblower Edward Snowden in 2013.

The judgment in the case brought against the United Kingdom, challenged both the system of bulk interception of cross-border communications set up by the UK, such as the Tempora programme, and the cooperation in bulk interception and surveillance with other countries. Most importantly among these countries are the so-called 'Five Eyes', i.e. the United States (using programmes such as UpStream and PRISM), Canada, Australia, New Zealand and the UK.

Given the complexity of the judgment, this blog article will limit itself to conveying the gist of the Strasbourg judges' ruling with regard to its findings on compatibility with Article 8 ECHR protecting the right to privacy, and to setting out some first impressions.

Overall, while the Court has provided some useful standards in relation to mass surveillance online, the judgment is affected by some key deficiencies that unfortunately limit considerably its contribution to provide a solution for the current human rights challenges in the digital sphere.

The Importance of Metadata for Today's Surveillance Practices

This much awaited judgment is a landmark ruling because the Court, for the first time, addresses the challenges of mass surveillance carried out not only on data but also on metadata. Metadata includes information left in the Internet such as the author of the information, the location, the subject, and other identifiers.

The Court recognizes that its jurisprudence of ten years ago or more, most of which is based on targeted surveillance on individual communications, cannot stand the test of the internet revolution, in which "lives are increasingly lived online" (para. 341). The Court recognises the centrality of metadata when dealing with the Internet, when it finds that "any intrusion occasioned by the acquisition of related communications data will be magnified when they are obtained in bulk." (para. 342).

The consequence of this finding, for the majority of the Grand Chamber, is that end-to-end safeguards are needed, i.e. from the moment of collection of the data or metadata until the moment of cessation of the surveillance activity on a given set of information. Further, these safeguards should increase as bulk interception progresses, based on the assumption that the more advanced it becomes, the closer it gets to the individual and to the content, hence to "traditional" surveillance.

Based on this reasoning, the Grand Chamber looks at “whether the domestic legal framework clearly define[s]:

1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual’s communications may be intercepted;
3. the procedure to be followed for granting authorisation;
4. the procedures to be followed for selecting, examining and using intercept material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; and
8. the procedures for independent *ex post facto*review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.” (para. 361)

Sharing Surveillance: How and When

The Court affirmed that “the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself” (para. 362). These are circumstances clearly set out in domestic law; ensuring that the transferring State has in place safeguards against abuse; heightened safeguards for material requiring special confidentiality; and independent control.

However, contrary to the standard set out in EU law and by the Court of Justice of the EU, “[t]his does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer” (para. 362).

Finally, where intelligence surveillance concerns the UK’s request to obtain information or to search for information in the data or metadata acquired and stored by a third country, the Court forcefully stresses that these systems must not result in any circumvention of the requirements it has set out (para. 497).Therefore, requests can only be made if there is a basis in domestic law, which must be accessible and foreseeable and with clear rules “which give citizens an adequate indication of the circumstances in which and the conditions on which the authorities are empowered to make such a request … and which provide effective guarantees against the use of this power to circumvent domestic law and/or the States’ obligations under the Convention” (para. 497). In addition, there should be independent supervision and *ex post facto* review. Once the information is received, the standards set out by the Court for surveillance carried out by a Contracting Party to the ECHR must be applied.

Big Brother Must Work

As is evident, the Court has set some innovative standards to apply the Convention's rights, in particular the right to privacy under article 8 ECHR, to the bulk interception of communications. However, a closer analysis of the judgment – and in particular the separate opinions – shows that this landmark ruling misses the mark in the era of Big Data.

First, the judgment is vitiated by an implicit but excessive trust in the intelligence services and in the Government's assessment that interception, storage, analysis and surveillance of data and metadata is essential to protect national security. The Grand Chamber's majority does not attempt to assess the veracity of this sweeping assertion by the UK, with an application of the tests of necessity and proportionality, but relies blindly on it. This is a conceptual weakness, because once this premise is accepted, the judges' reasoning builds on the primary need to make mass surveillance work.

Secondly, while the criteria established are useful and in part an improvement on its previous requirements, the Court has mostly conducted an assessment of the UK regulatory framework rather than of its actual functioning in practice, to the point that the Court found the existence of a legislation merely prohibiting the "circumvention of guarantees" to be an effective system to ensure that there is no circumvention of guarantees (see para. 513).

Thirdly, it is problematic that some of the Court's criteria for allowing for bulk interception can be overridden if, "when viewed as a whole, sufficient guarantees against abuse are built into the system to compensate for this weakness" (para. 370). This exception brings a degree of unpredictability to the system that in itself defeats the need to set out clear grounds for bulk interception. Both States and the Court are therefore allowed to carry out a case-by-case assessment for any kind of surveillance.

Fourth, one of the requirements of the legal framework gives up an essential guarantee of human rights protection, namely the oversight by the judiciary. While requiring that an independent authority be involved in the authorisation and *ex post* control processes, the Grand Chamber's majority explicitly excludes that this must be a judicial authority and allows for "internal" authorities to be envisaged, even if they must be, at least on paper, "independent of the executive" (para. 359). On this specific point, the Court of Justice of the EU took a stronger position requiring the involvement of a judicial authority (see, Schrems II judgment, paras. 186-194).

With regard to foreign intelligence– whether the UK allows foreign intelligence services to obtain communications or the UK obtains or requests communications from foreign services – the Court applies lower standards and does not adopt the protection equivalency system that is provided by EU law. This means that it will be easier for the UK to request information from, for example the US National Security Agency, than to acquire it itself, with the only defence for privacy being an a priori faith in the letter of UK law, which states that "circumventing" national procedure is prohibited.

Finally, the Strasbourg judges have clearly avoided the central question of how to regulate forms of close transnational surveillance cooperation, such as that of the Five Eyes, that nurture and dispose of entire databases containing a high amount of the data produced on the Internet.

Too Late and Too Little

In conclusion, although the Grand Chamber's ruling made modest advances in protecting human rights on the internet, overall it missed the opportunity presented by this case to address the technological revolution of the last decade, namely Big Data.

The Court has recognised the danger, but the solutions it has posited are still based on the logic of targeted surveillance systems, according to which the level of human rights protection should increase the more the surveillance is closer to the individual. Based on this logic, the more a CCTV camera closes on you the more guarantees you should have to protect your right to privacy.

However, the current Big Data system resembles more to an infinite set of cameras installed in everyone's houses, which intelligence services can access on demand. The failure by the Court to recognise and effectively regulate the moment of data gathering risks being fatal to the capacity of the guarantee established by the Court to effectively protect the human rights of people subject to this kind of surveillance.

It is to be hoped that the Court will revisit its jurisprudence in future cases to more effectively ensure that its jurisprudence provides effective protection to human rights in relation to the challenges brought by the technologies of today and not those of the past.

Disclaimer: The author is Senior Legal Advisor to the International Commission of Jurists (ICJ), which has intervened as a third party in the proceedings described.
